A Better MPLS Network With Meraki MX Security Appliances

July 2012

This whitepaper describes how to reduce costs, improve efficiency, and increase the reliability of traditional MPLS networks using the Meraki MX line of Security Appliances.

Copyright

© 2012 Meraki, Inc. All rights reserved.

Trademarks

Meraki® is a registered trademark of Meraki, Inc.

www.meraki.com

660 Alabama St.
San Francisco, California 94110

Phone: +1 415 632 5800
Fax: +1 415 632 5899

1 Executive summary

The Meraki MX Security Appliances provide indispensible features like WAN optimization, failover, traffic shaping and Layer 7 security for organizations that use MPLS, as well for those who are looking to transition away from MPLS to regular ISP-based connectivity.

2 Challenges with MPLS

MPLS is a popular access technology among enterprise networks. Key benefits include guaranteed service level agreements (SLAs), latency caps, low jitter and high availability. In addition, MPLS allows IT departments to outsource complex WAN termination and routing challenges to service providers. Typically, companies running latency-sensitive, mission-critical applications over their network choose MPLS-based connectivity for their branches. For example, a large number of multi-site VoIP deployments run on MPLS networks.

On the other hand, some of the major IT initiatives like BYOD, guest networking, and cloud based services make it increasingly difficult and expensive to run large distributed networks on MPLS.

2.1 Cost of bandwidth

A major drawback of MPLS is the bandwidth cost. For instance, in North America low cost 5-20Mbps connectivity is widely available however many existing MPLS deployments continue to run on 1.5 Mbps T1 or fractional T1s due to cost concerns. With the recent popularity of guest networking and BYOD initiatives, it is becoming increasingly difficult to run a branch on 1.5 Mbps.

2.2 Excess Latency

MPLS was designed for the era of centralized IT, where all branch connections terminated via a full-tunnel connection to the HQ or the datacenter before breaking out to the Internet. This was the suitable architecture when all security, compliance and monitoring services (e.g., web/content filtering) could be deployed centrally at the HQ / datacenter, inline between the branch traffic and the Internet.

However, with the IT world transitioning to cloud based services and taking advantage of SaaS offerings like Salesforce.com, Google Apps or Dropbox storage, the aging, centralized full-tunnel architecture is no longer viable. Most SaaS providers have optimized their infrastructure to provide low-latency access to their

services, regardless of the end-user's geography. But the so-called trombone[1] architecture adds unnecessary latency and complexity since it forces traffic to travel all the way to the HQ / datacenter before going back to the SaaS provider. In some cases, the round-trip delays can exceed 100 ms for Internet access. The full-tunnel MPLS topology adversely impacts end-user productivity and increasingly becomes a bottleneck and a single-point-of-failure.

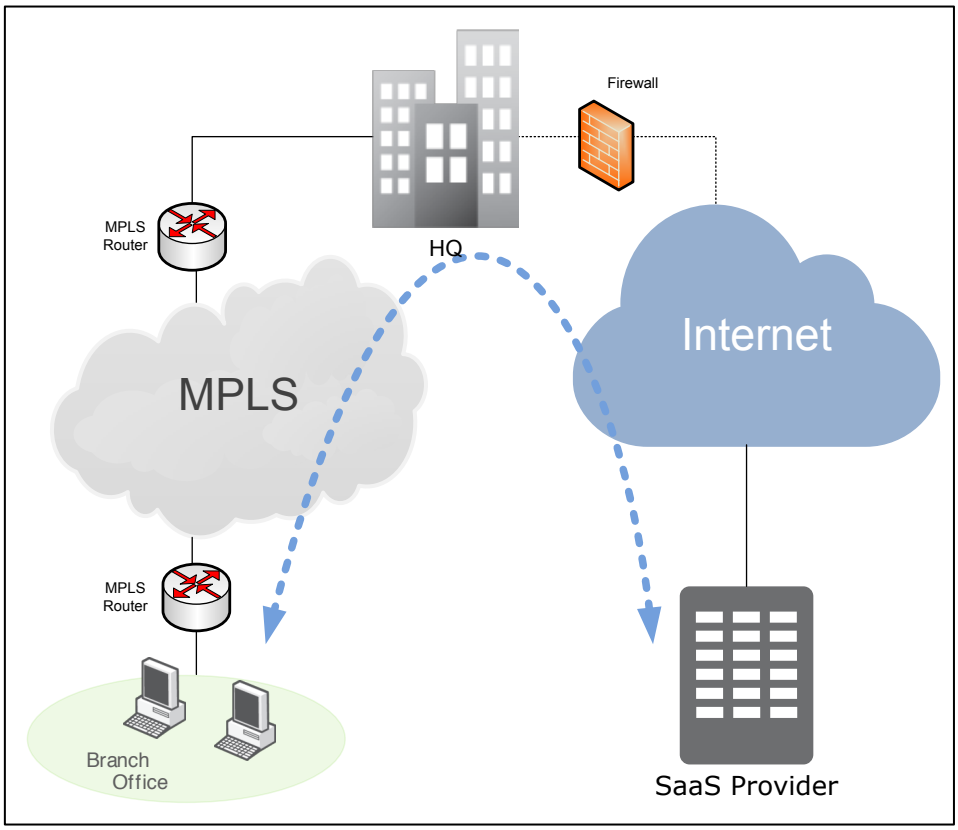


Figure 1 - Full-tunnel MPLS adds latency to Cloud applications.

1 In a trombone architecture, the traffic flows from the branch to a faraway datacenter, then back to the SaaS provider on the Internet.

3 Adding the MX to common MPLS architectures

The Meraki MX can reduce the cost and complexity of barebones MPLS deployments in a number of ways, depending on the MPLS architecture. Two common network architectures are worth highlighting. The first is the full-tunnel MPLS, where all the local network traffic goes through the datacenter before breaking out to the Internet. Alternatively, MPLS networks can be augmented with a local ISP connection for failover and/or guest Internet access purposes.

Below is a summary of all the networking and security features of the MX security appliances and their applicability for the two MPLS deployment use-cases above.

	WAN optimization	Layer 7 visibility	Layer 7 traffic shaping	WAN failover	Layer 3/7 security	Auto VPN routing
Full-tunnel MPLS	✓	✓	✓			
MPLS+ISP connection	✓	✓	✓	✓	✓	✓

3.1 Full-tunnel MPLS

Full-tunnel MPLS is a special case of the hub-and-spoke model, where all the branch traffic goes to the datacenter before breaking out to the Internet.

In this network topology, the MX is deployed at every branch for WAN optimization and traffic shaping. WAN optimization reduces latency and bandwidth utilization. Traffic shaping and prioritization throttles recreational traffic, while guaranteeing minimum bandwidth availability for the mission-critical traffic.

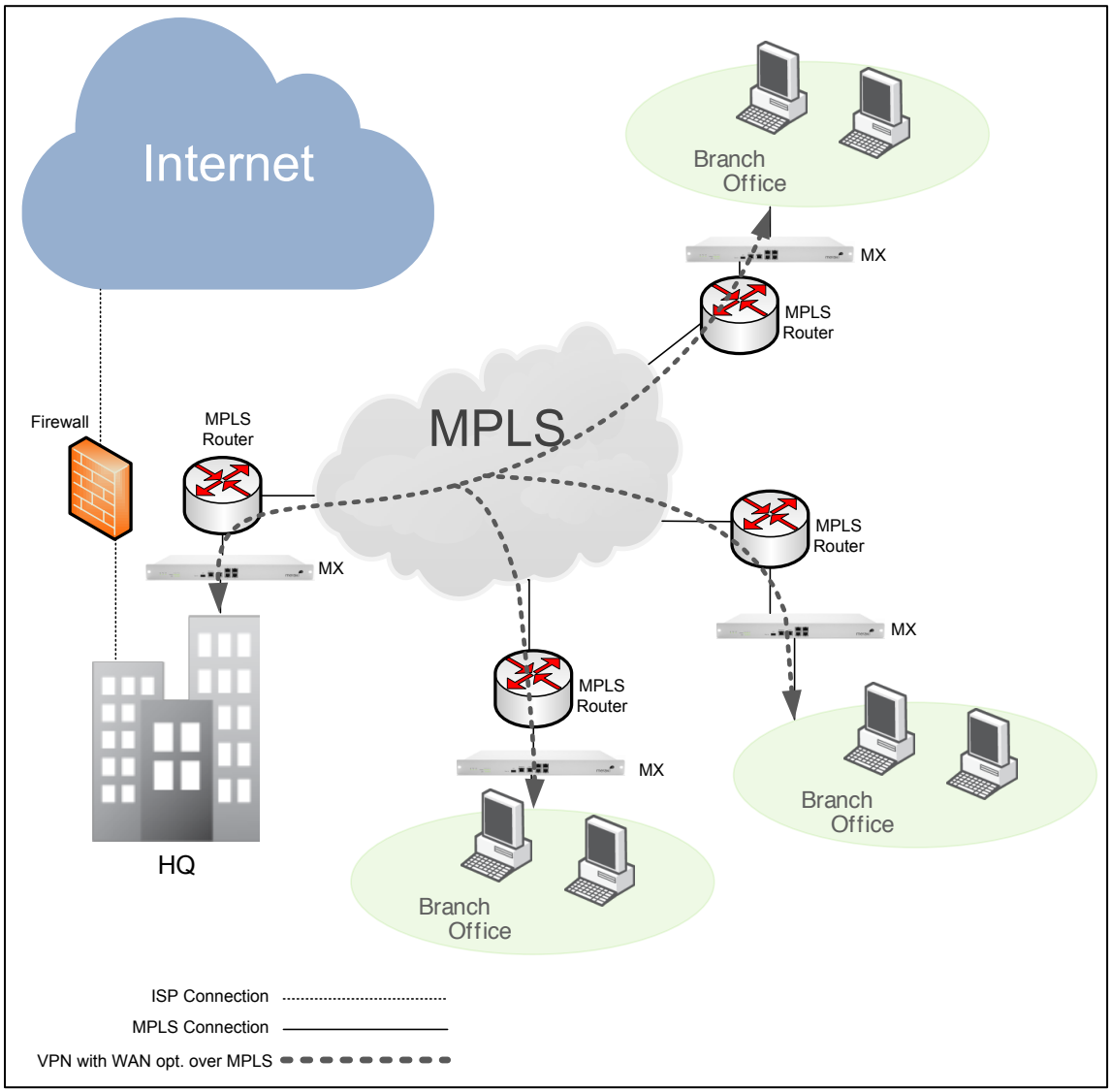


Figure 2 - MX in passthrough mode for WAN optimization and traffic shaping

3.2 MPLS plus local ISP connection

In this network topology, each branch has one MPLS link and one or more low-cost ISP connections, e.g., DSL, cable or 3G/4G. The MX provides WAN failover, Layer 3/7 security services for the non-MPLS connection, WAN optimization, and traffic shaping.

Also, the second ISP line is a great solution for handling guest Internet access, as opposed to sending the guest traffic over the MPLS to the datacenter.

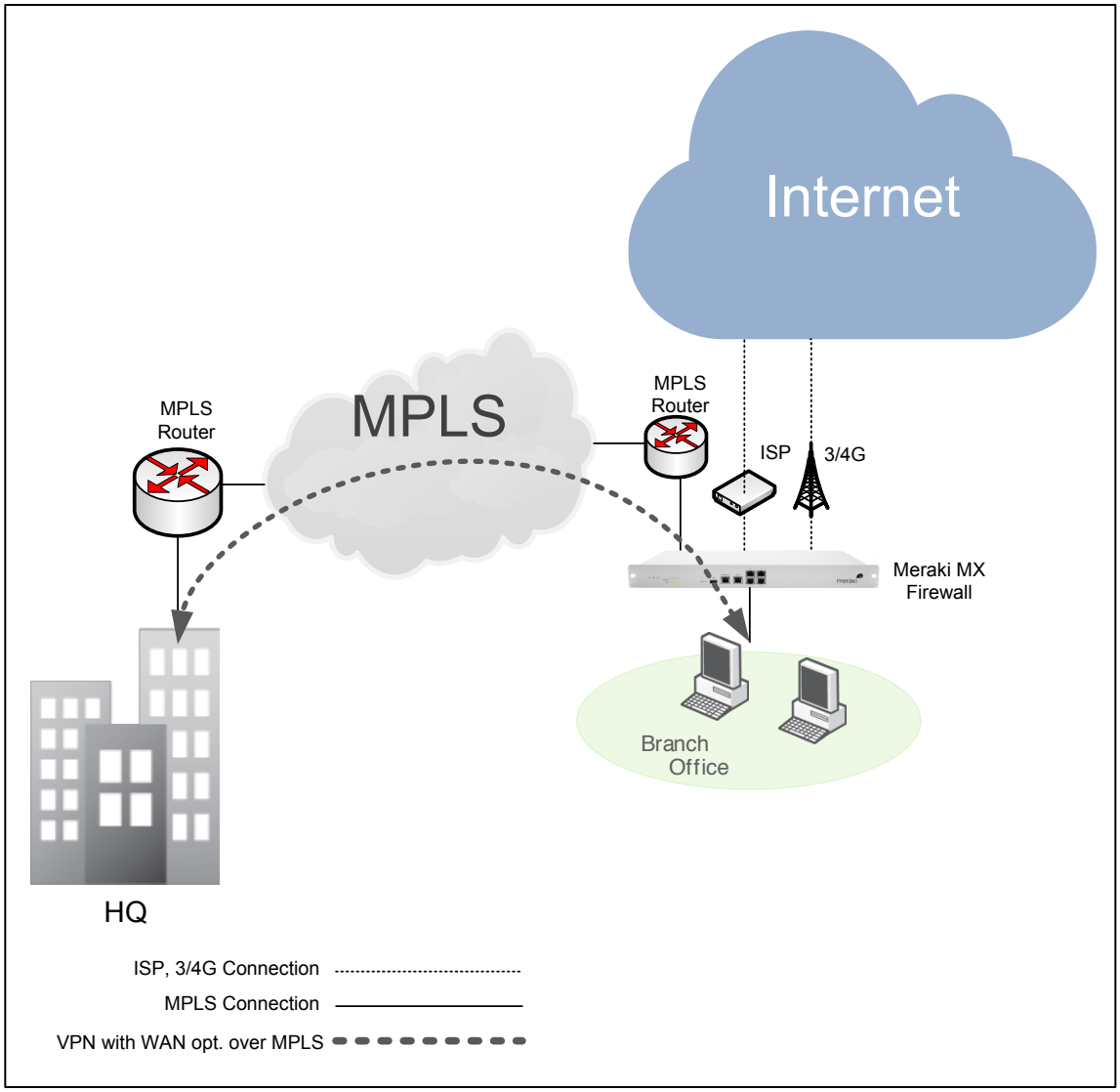


Figure 3 - MX as the branch firewall

4 Benefits of the MX security appliances

The MX Security Appliances offer a wealth of Layer 3/7 traffic optimization and security features that alleviate the bandwidth limitations and latency challenges across all types of MPLS deployment topologies. Key features include:

- WAN optimization.
- WAN failover and load balancing.
- Layer 3 and Layer 7 security at the edge.
    - Stateful firewall.
    - Local DHCP service for guest access.
    - Content filtering.
    - Anti-virus and anti-phishing engine.
    - IDS / IPS engine.
- Automatic routing and VPN for WAN failover.
- Traffic visibility and shaping for mission-critical services.

4.1 WAN optimization

Meraki's built-in WAN optimization solution reduces the perceived latency between branches and the datacenter. WAN optimization uses a set of techniques to minimize the effects of network latency and, in the process, increase the network bandwidth.

4.1.1 Byte-level caching

The Meraki MX Security Appliances perform byte-level caching of content that is flowing between peer devices. That way, when a network client in a remote branch is trying to access the same data through the network, the data can be served locally from the MX.

Byte-level caching offers superior performance compared to object-level caching. Modifications to files do not trigger full content retransmissions, as the Meraki WAN optimization technology is sophisticated enough to transfer only the changed data across the WAN and reconstruct the modified file locally at the destination.

4.1.2 TCP compression

In addition to the byte-level caching, MX WAN optimization also compresses all TCP communications. Typically, TCP compression alone yields an additional 30% traffic reduction, which lowers

perceived latency between locations and improves WAN throughput.

4.1.3 Protocol optimization:

Many data transport protocols like HTTP, CIFS and FTP have been designed for local networks with low-latency and high data-loss. However, most MPLS deployments today exhibit the reverse behavior with low data-loss and high-latency (particularly for global networks).

Protocol optimization algorithms improve the performance of these transport mechanisms by eliminating unnecessary round-trip signaling messages and other "chatty" handshaking methods.

4.2 WAN failover and load balancing

The MX provides both WAN failover and load balancing. Typically, the MX is configured to provide VPN between a branch and the HQ. In addition, enabling split-tunneling allows the MX to provide load balancing and link failover across heterogeneous links, e.g., MPLS, cable, DSL, and 3G/4G.

4.2.1 Failover via a local ISP connection

The MX Appliance switches the WAN connection over to the secondary uplink in the event of a Layer 2 or 3 failure detection. The detection algorithm contains a hysteresis feature that dampens unnecessary switches back and forth in case a link is "flapping".

4.2.2 Failover via a 3/4G cellular modem

Similar to the regular failover mechanism, the MX can also use a 3/4G cellular modem as a backup connection. Note that if the network already has an ISP backup link, the 3/4G connection will be used as a secondary backup connection, further increasing network reliability.

4.3 Layer 3 and Layer 7 security at the edge

Many organizations leverage the secondary Internet connection for local guest network access. For others, the secondary link is only active during the failover mode. In either case, it is important to provide a complete suite of security features at the branch edge to eliminate potential network vulnerabilities.

4.3.1 Stateful firewall

All Meraki MX Security Appliances offer a feature-complete stateful firewall, including support for DMZ, 1:1 NAT and other traditional Layer 3 security capabilities.

4.3.2 Local DHCP service for guest access

Meraki MX Security Appliances have a fully-configurable per-VLAN DHCP service, ideal for enabling guest networking access.

4.3.3 Content filtering

The Meraki MX Security Appliance features a robust URL / content filtering engine that uses the latest database from Webroot's BrightCloud content categorization engine, including over 82 categories with more than one billion URL entries. The categories and database are automatically updated from the Meraki dashboard.

4.3.4 Anti-virus and anti-phishing engine

The MX also provides anti-malware and anti-phishing protection using Kaspersky's flow-based detection technology. The signatures are updated every hour and provide protection against phishing URLs, malicious executable files and scripts, and other malware.

4.3.5 Intrusion detection and prevention (IDS / IPS)[2]

To ensure compliance (e.g. PCI) and security, the MX also provides a Snort based intrusion detection and protection engine. Similar to the other security engines, the Snort rules are automatically updated from the Meraki dashboard.

4.4 Automatic routing and VPN over MPLS for WAN failover

The MX Security Appliance features Auto VPN, a patent-pending Meraki technology that automates the discovery and distribution of routes across all MX peers, as well as the creation of secure IPsec VPN tunnels.

Auto-VPN:

- Provides an additional layer of security through VPN encryption.
- Automatically updates and self-configures VPN tunnels in the event of an IP address, or topology change.

[2] Meraki's IPS / IDS engine is scheduled to be available in Q4 2012

- Uses standard IPsec and is interoperable with 3rd party concentrators.

4.5 Traffic visibility and shaping for mission-critical services.

Meraki MX Security Appliances use Layer 7 deep packet inspection techniques to fingerprint devices and traffic. By deploying MX Security Appliances, administrators can create traffic priority queues for mission critical applications, throttle or eliminate unwanted applications, and block users who violate IT / HR policies, a common concern for networks with guest access.

5 Auto VPN considerations

Deploying MX Security Appliances in MPLS networks uses the Auto VPN service. It is agnostic to the uplink connectivity type, e.g., MPLS, cable, DSL, and 3G/4G. The Auto VPN service is enabled on the MX's primary uplink by default, with automated failover to any redundant links in the event of primary link failure.

5.1 Auto VPN routing

Unlike traditional gateway solutions which require a routing protocol like OSPF, BGP or EIGRP over VPN, Auto VPN uses the information already available in the Meraki dashboard about various networks and automatically builds route maps for each MX device, based on their WAN IP, local subnets, static routes and VPN peers.

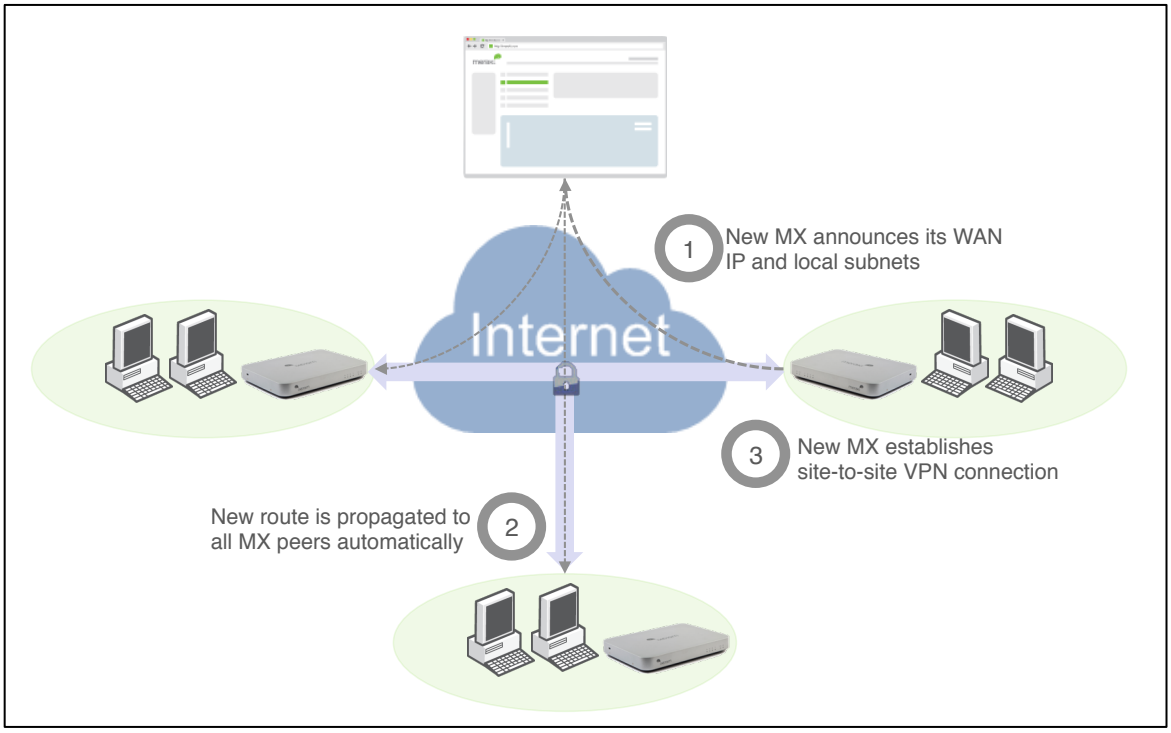


Figure 4 - Automatic route distribution and VPN connectivity.

5.2 Auto VPN overhead

Decoupling the WAN connectivity from the local area network has significant benefits, as outlined in the next section. But it also comes with an overhead. Establishing an IPsec VPN over MPLS adds

latency and reduces total payload and it is import to put these two tradeoffs in context

- Added latency: less than 4 ms (RTT).
- Added overhead: 68 bytes per packet.

For example, an inter-office VoIP call using the G.729 codec, with 50 packets per second, would generate 27.2 kbps additional IPsec traffic, less than 2% overhead for a T1 MPLS line with 1.544 Mbps symmetrical throughput.

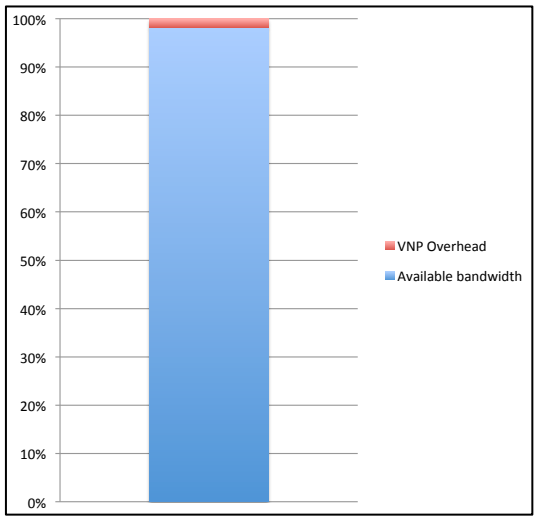


Figure 5 - For a G.729 VoIP call over 1.5 Mbps, the overhead is 1.8% per call.

5.3 Auto VPN benefits:

The Auto VPN simplifies branch routing, security, and failover configuration by way of abstracting the uplink connections from the local branch network settings.

- WAN connection becomes agnostic. MPLS, standard ISP uplink, or 3/4G all work the same way.
- Auto VPN provides an additional layer of security through encryption.
- Auto VPN automatically updates and self-configures VPN tunnels in the event of an IP address, or topology change.
- The Internet traffic can be load-balanced.
- VPN connections are standard 128-bit AES IPsec connection between peers and don't traverse the Meraki cloud infrastructure.

5.4 Auto VPN monitoring

Site-to-site VPN

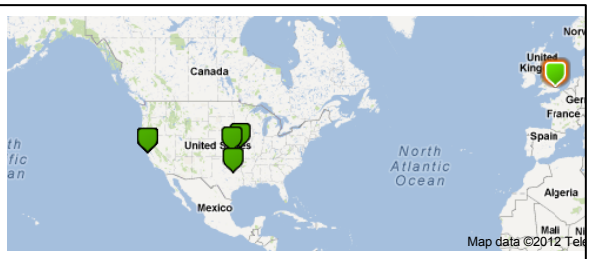
Connection status for Ikarem Corp - Firewall

Configuration: This device is exporting 4 subnets over the VPN: 172.16.20.0/24, 172.16.30.0/23, 172.16.40.0/24, 172.16.80.0/24.

VPN Registry: Connected. This MX was able to connect to multiple VPN registries using UDP port 9350.

NAT type: None (Public IP). This MX has a publicly accessible IP address and is using 208.90.213.100:57963 as a contact point.

Encrypted. Using IPsec and AES encryption.



Site connectivity

Location	Subnet(s)	Status*	Latency (RTT)	Last heartbeat
Branch #1	10.128.1.0/24 172.16.20.0/24	connected	15.72ms	1 second
Ikarem Corp - Firewall	172.16.30.0/23 172.16.40.0/24 172.16.80.0/24	-	-	-
Branch #2	192.168.1.0/24	connected		4 seconds
Branch #3	10.3.3.0/24	connected	11.43ms	8 seconds
Branch #4	10.128.2.0/24	connected	22.16ms	2 seconds
Branch #5	10.128.3.0/24	device offline		
Branch #6	10.1.0.0/16	connected	9.87ms	5 seconds
Branch #7	10.128.4.0/24 10.128.5.0/24	connected	14.37ms	5 seconds
Branch #8	10.0.20.0/24 10.0.21.0/24 10.0.30.0/24 10.0.31.0/24	connected	147.54ms	6 seconds
Branch #9	10.128.6.0/24	connected	15.86ms	10 seconds
Branch #10	10.128.7.0/24	connected		1 second

Figure 6 - Real-time connectivity monitoring.

The Auto VPN provides a resilient inter-connected network grid that adapts to topology changes and failures with rapidly converging route maps and VPN tunnels that reestablish within seconds. The entire Auto VPN network can be monitored in real-time from the Meraki dashboard.

6 Conclusion

Meraki MX security appliances can decrease the costs associated with increasing MPLS capacity by squeezing more out of existing MPLS bandwidth and also enabling the use of standard ISP circuits.

In addition, centralized control of geographically distributed networks through the Meraki dashboard makes it easy to implement the MX consistently across many locations.

Combining the WAN optimization, failover, traffic shaping and Layer 3/7 security features, administrators can maximize their MPLS deployments by:

- Reducing latency and increasing bandwidth with WAN optimization.
- Improving uptime by adding an ISP link and/or a 3/4G cellular modem for failover.
- Efficiently using scarce MPLS bandwidth by sending only mission-critical traffic through the MPLS tunnel.
- Providing security and compliance services with anti-virus, anti-phishing, intrusion detection/prevention and content filtering.

Lastly, the Meraki MX Security Appliances also afford the opportunity to completely migrate away from MPLS to regular ISP connections (with multiple circuit providers) to maintain reliability at a fraction of the MPLS total cost of ownership.

You can learn more about Meraki MX Security Appliances at http://www.meraki.com/mx.